EXHIBIT 11

(May 12, 2023 Declaration of
Nicholas Del Rosso)

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 1:21-MC-6

In re Application of KARAM SALAH AL DIN AWNI AL SADEQ and STOKOE PARTNERSHIP SOLICITORS for an Order Under § 1782 to Conduct Discovery for Use in Foreign Proceedings.	)	**DECLARATION OF NICHOLAS DEL ROSSO**

I, **Nicholas Del Rosso**, do hereby declare under penalty of perjury pursuant to 28 U.S.C. § 1746 the following:

1. I am the president and owner of Vital Management Services, Inc. ("VMS"), a North Carolina corporation.

2. I am over the age of eighteen and am competent to testify as to the matters set forth in this Declaration.

3. Karam Salah Al Din Awni Al Sadeq ("Mr. Sadeq") and Stokoe Partnership Solicitors' ("Stokoe"; collectively "Applicants") *Ex Parte* Application (the "Application") is predicated on a false premise, false evidence, and misrepresented allegations that there are similarities between Applicants' hacking claims and the now dismissed hacking claims brought against me and

my company by Farhad Azima ("Mr. Azima"). *See, e.g., Azima v. Del Rosso, et al.*, No. 20-cv-954 (M.D.N.C. Oct. 15, 2020) (the "MDNC Lawsuit").[1]

4. On June 21, 2019, I signed and submitted a (First) Witness Statement of Nicholas Del Rosso in support of the Claimant, the Ras al Khaimah Investment Authority ("RAKIA"), in its fraud lawsuit against Mr. Azima in the High Court of Justice in London, Claim No. HC-2016-002798 (the "English Proceeding"). My First Witness Statement provided the relevant background of my engagement by Dechert LLP ("Dechert") with respect to its representation of the Government of Ras al Khaimah ("RAK") and its entities. My First Witness Statement also provided the factual background for my limited involvement in the retrieval of data appearing to relate to Mr. Azima, after its public availability had been discovered by others. I have since re-affirmed my First Witness Statement in the MDNC Lawsuit. *See Azima v. Del Rosso, et al.*, No. 20-cv-954, at D.E. 132-1 (M.D.N.C. Jan. 30, 2023). A true and accurate copy of my June 21, 2019 (First) Witness Statement of Nicholas Del Rosso is attached hereto as **Exhibit A**.

5. On February 22, 2021, I signed and submitted a Second Witness Statement of Nicholas Del Rosso in the English Proceeding. My Second Witness Statement provided further background on my lawful work with

[1] Mr. Azima's hacking claims in the MDNC Lawsuit were dismissed as time-barred. *Azima v. Del Rosso, et al.*, No. 20-cv-954, at D.E. 65 (M.D.N.C. Dec. 10, 2021).

CyberRoot Risk Advisory Private Limited ("CyberRoot") on behalf of several clients, including but not limited to Dechert. In my Second Witness Statement, I provided an explanation for each of the payments to CyberRoot raised by Mr. Azima in the English Proceeding, which I confirmed (1) did not concern Mr. Azima; and (2) did not involve any instructions to hack anyone or disseminate material obtained through hacking. I have since re-affirmed my Second Witness Statement in the MDNC Lawsuit. *See Azima v. Del Rosso, et al.*, No. 20-cv-954, at D.E. 132-1 (M.D.N.C. Jan. 30, 2023). A true and accurate copy of my February 22, 2021 Second Witness Statement of Nicholas Del Rosso is attached hereto as **Exhibit B**.

6. Throughout June 2020 and July 2020, I had several conversations with Yuri Koshkin ("Koshkin"), who I understood had approached me on behalf of the Eurasian Natural Resources Corporation's ("ENRC"). During those conversations Mr. Koshkin advised me about the involvement of ENRC in all of these related matters. Among other things, Koshkin advised me that he had learned from another individual acting on behalf of ENRC, Dmitry Vozianov, that the ENRC was funding Mr. Azima's appeal in the English Proceeding because they had committed to paying his judgment; that the ENRC was funding Mr. Sadeq's litigation; and that Mr. Azima requested funding for two new lawsuits (and that, at that time, the ENRC declined to fund new lawsuits). It is my understanding that the two lawsuits that Mr. Azima requested

funding for in June 2020 were the cases brought against me and others: the MDNC Lawsuit and *Azima v. Dechert LLP, et al.*, No. 22-cv-8728 (S.D.N.Y. Oct. 13, 2022).

7. I reaffirm my prior sworn statements in the English Proceeding and the MDNC Lawsuit. For the avoidance of doubt, I did not hack Mr. Azima's devices or cause him to be hacked, and I do not know who obtained copies of information and data allegedly belonging to Azima, or how such material was obtained. Similarly, I did not upload his data or information to the internet or cause such data or information to be uploaded, and I do not know who uploaded his data or information.

8. Further, for the avoidance of doubt, neither I nor VMS received funds or used our respective financial accounts or other methods of payment to facilitate the hacking or republication of any data or information allegedly hacked from Mr. Azima. Similarly, neither I nor VMS received or transferred funds, extended credit, or otherwise paid other persons or companies to facilitate the hacking of or republication of Mr. Azima's data or information.

9. In addition, for the avoidance of doubt, I did not hack Applicants' legal team or cause them to be hacked, and I do not know who, if anyone, hacked them. Neither I nor VMS received funds or used our respective financial accounts or other methods of payment to facilitate the hacking of Applicants' legal team. Similarly, neither I nor VMS received or transferred

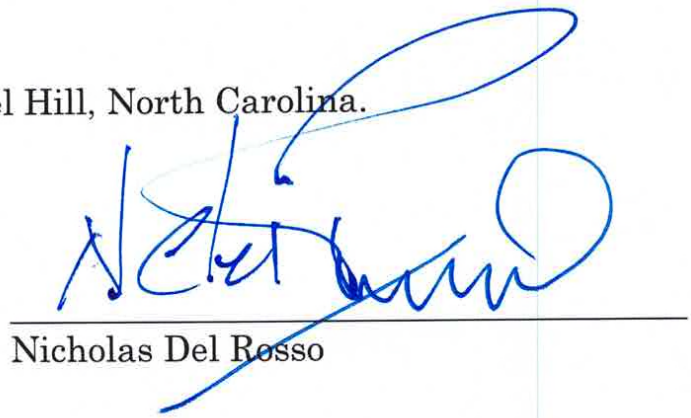
funds, extended credit, or otherwise paid other persons or companies to facilitate the hacking of Applicants' legal team.

10. Finally, it is my understanding that Applicants' request pursuant to 28 U.S.C. §1782 is based on allegations that I caused another company, CyberRoot Risk Advisory Private Ltd. ("CyberRoot"), to hack data from Applicants, Azima and possibly others. This false allegation is based on bank records obtained from CyberRoot's bank account in India. At no time did I authorize the release of any such bank records, and had no authority to release such records in any event. It is my understanding that those bank records were obtained by Applicants after a now-terminated bank employee stole them, after receiving a bribe.

11. For the avoidance of doubt, the payments reflected in the records contain nothing to indicate that I have any knowledge or information that would support the allegation that I (or VMS) paid CyberRoot to hack any of the Applicants, or Mr. Azima. I have no knowledge that CyberRoot hacked any of those individuals or affiliated entities, and, in fact, neither I nor VMS ever worked with CyberRoot on any work related to the Applicants. Similarly, neither I nor VMS ever paid CyberRoot for any work related to the Applicants.

12. I declare under penalty of perjury that the foregoing is true and correct pursuant to 28 U.S.C. § 1746.

Executed on May 12th, 2023 in Chapel Hill, North Carolina.



Nicholas Del Rosso

EXHIBIT A

(First Witness Statement of
Nicholas del Rosso)

Claimant
Nicholas del Rosso
First
June 2019

IN THE HIGH COURT OF JUSTICE **Claim No. HC-2016-002798**

BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES

BUSINESS LIST (ChD)

BETWEEN:

RAS AL KHAIMAH INVESTMENT AUTHORITY

Claimant

-and-

FARHAD AZIMA

Defendant

WITNESS STATEMENT OF NICHOLAS DEL ROSSO

I, **NICHOLAS DEL ROSSO**, of 1340 Environ Way, Chapel Hill, North Carolina, 27517 USA **WILL SAY** as follows:

1. I am the President and owner of Vital Management Services Inc. of the above address ("**VMS**"). VMS provides consulting services to law firms and businesses engaged in investigating or evaluating suspected fraud. I make this witness statement at the request of the Claimant, Ras Al Khaimah Investment Authority ("**RAKIA**").

2. Save insofar as is stated otherwise, the facts set out below are within my own knowledge or are derived from other sources or documents that I have seen and which in all cases I believe to be true. Where any facts are not within my knowledge, the source of those facts is stated.

3. As some time has elapsed, I do not have a precise recollection of the exact dates and times certain of the events I refer to occurred. I have refreshed my memory by reference to emails that I sent or received in the relevant period. I refer to some of these documents below by reference to their disclosure ID number (contained in curly brackets { }).

4. In August 2014, VMS was engaged by Dechert LLP to investigate assets potentially stolen from the Government of Ras Al Khaimah ("**RAK**"). Pursuant to its engagement VMS examined potential frauds committed by, amongst others, Khater Massaad. I took my instructions from Dechert LLP, and had limited direct contact with Jamie Buchanan and other representatives of the RAK government. I had worked previously with other lawyers then at Dechert LLP on unrelated matters involving suspected fraud.

5. In early August 2016, I received a telephone call from Neil Gerrard of Dechert. During that call, Neil told me that Stuart Page had identified two links on the internet which appeared to contain data relating to Farhad Azima, an associate of Khater Massaad. I do not know Stuart Page but I had heard of him because he works in a similar industry to me.

6. When Neil and I spoke, he asked if VMS could assist in retrieving the data that had been found, or if VMS could engage a suitable forensic data specialist to do so. He then dictated to me over the phone the details of the two links where the information could be found. I do recall Neil warned me that the material could contain viruses.

7. I do not recall the exact date of this call but I do remember that it was very early in the morning in North Carolina where I live. Neil knows that I get up early. I also recall that I set things in motion the same day. I saw this as a

commercial opportunity and I was concerned that Neil might have also asked others if they could access the material. I have seen an email from me to Rich Garcia at Northern Technology, Inc. ("**NTi**") (which was later engaged to download the material as explained below) timed at 10.28am on 9 August 2016 referring to an introductory call **{RAK0001941}**. I think that I would have sent the email shortly after receiving Neil's call, which I believe must therefore have been on 9 August 2016.

8. Chris Swecker is a former Assistant Director of the FBI and VMS's attorney. I regularly instruct subcontractors through Chris to ensure that engagements are properly documented and so that, where applicable, legal privilege is maintained. Following Neil's call, I called Chris to ask for recommendations of who might be able to help download this material, given the warning about viruses that Neil had given me. Chris recommended that I contact Rich Garcia at NTi. I believe that Chris mentioned other potential experts but was concerned that this project might be too small a piece of work for some of the more prominent companies engaged in cyber matters. I also understand that Rich Garcia, who was the CEO of NTi, and Chris had worked together at the FBI.

9. Following Chris's recommendation, I spoke to Rich Garcia. Rich Garcia told me that NTi had the necessary expertise I was looking for. I have seen an email exchange between me and Chris starting at 11.47am on 9 August 2016 which confirms that VMS sought to engage NTi immediately **{RAK0001944}**.

10. In that email I confirm to Chris that I had given Rich the two web addresses: https://thepiratebay.org/torrent/15484452 and https://monova.org/42248895. These were the addresses that Neil had given to me in our phone conversation. I note that my email says that I had told Rich that "*as recently as last week – we were advised by researchers that a deep web search indicated that data relating to Farhad Azima was on a site…*" and that "*In addition, over this past weekend, we were told that another site…*". I recall that these statements were reports of information that Neil had told me during our call.

11. I have seen an email from me to Chris Swecker on 12 August 2016 at 7.54pm in which I provide him with two additional sites from a Google search referring to "*Farhad Azima of the Aviation Leasing Group Exposed*" **{RAK0001946}**. These were Google searches that I had performed myself, earlier that day. I assumed the content of these new sites was related to the two original sites that Neil had given me.

12. I have seen an email exchange between Neil Gerrard and I on 15 August 2016 which starts with Neil stating "*I've had another call from Stuart who confirms again that there is a website on FA. He seems to think it's been generated from a UAE source. I've asked for details…*" **{RAK0001949}**. I responded confirming that VMS had instructed NTi to search and recover what may have been on them. I also asked how it was known that the site was set up in the UAE. Neil confirmed in response that he did not know and that he would ask. I do not recall ever following up this inquiry with Neil or hearing more from him on where the sites might have originated from.

13. On Tuesday 23 August 2016 at 9.33am I received an email from Rich Garcia confirming that NTi would provide some of the data to me by Wednesday **{RAK0001958}**. He explained some of the difficulties of downloading data from this particular torrent file. I had no prior knowledge of or experience with such things.

14. I received a follow up email later that day from Rich confirming that his analyst Jess Gray had been successful with the download and could provide the material on some type of secure "drop box" file **{RAK0001959}**. In fact NTi sent me a drive by FedEx as was confirmed in an email the following morning on 24 August 2016 **{RAK0001962}**. I was flying to London that day for a meeting at Dechert so I had the drive delivered to me together with a copy for Dechert. I do not recall who I gave the copy to at Dechert. It would have been either Neil Gerrard or one of his associates.

15. I have seen an email dated 1 September 2016 from me to Chris Swecker, Rich Garcia and Jess Gray at 7.46am entitled "*Update – New Data*"

{RAK0001980}. In this email I state that the "*client's 'spotter' in Dubai has reported a new data dump.*" I do not clearly recall how I learned of this but I believe it was Neil or one of his associates who told me. I do not remember being told the identity of the "*spotter*". I assumed it was a reference to Stuart Page. I note that in this email I also referred to another "*message*" and explained that I could not open it (due to lack of signal) to give them the link. I do not recall the means by which I received the other "*message*" but, after a thorough search of my documents and devices, I have not found any records matching its description.

16. The following day on Friday 2 September 2016 at 10.21am I sent a further email to Jess Gray, Rich Garcia and Chris Swecker providing them with details of the additional sites I had received: seedpeer.eu/details/11679969/Fraud-between-Farhad-Azima-and-jay-Solomon.html and 1337x.to/torrent/1756315/Fraud-between-Farhad-Azima-and-Jay-Solomon.html **{RAK0001982}**. Again, I described these as having come in from Dubai. I believe that was a reference to them having possibly come from Stuart Page, who I believed to be based in the UAE.

17. On 8 September 2016 Jess Gray confirmed to me by email that she had been able to download the data from "*the newest torrent release*" **{RAK0001966}**. She confirmed in this email that she would provide the new data on drives. I do not recall exactly how these drives were delivered to me or Dechert.

18. On 9 September 2016 I received a further email from Jess Gray confirming that she had received an alert about a new torrent data dump **{RAK0001970}**. I responded to her email querying whether this was a different set of data from the one she had recently downloaded. I also gave her instructions to begin the process of retrieving it from the web. She responded to confirm that it was "*an entirely new data dump*". On the same day I informed Neil Gerrard by email about NTi's discovery and confirmed that I had instructed NTi to try to recover the new set of data **{RAK0001972}**.

19. NTi were able to download and preserve this further cache of data that they had identified. I know that at some point NTi made the third tranche of data available to me but I do not recall exactly when or how.

20. I understand that Mr Azima alleges that RAKIA is responsible for hacking his computers and uploading his data to the internet. For the avoidance of doubt, I did not hack Mr Azima's computers, cause him to be hacked or know who hacked him. I did not upload his data to the internet, cause his data to be uploaded or know who did upload his data.

STATEMENT OF TRUTH

I believe that the facts stated in this Witness Statement are true.

Signed.....

NICHOLAS DEL ROSSO

Date: June 21, 2019.

EXHIBIT B

(Second Witness Statement of
Nicholas Del Rosso)

Respondent/Claimant
N del Rosso
Second
Exhibit NDR1
22 February 2021

IN THE COURT OF APPEAL **APPEAL REF: A3/2020/1271**
ON APPEAL FROM THE HIGH COURT OF JUSTICE HC-2016-002798
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
BUSINESS LIST (ChD)

BETWEEN:

RAS AL KHAIMAH INVESTMENT AUTHORITY
Respondent/Claimant

- and -

FARHAD AZIMA
Appellant/Defendant

SECOND WITNESS STATEMENT OF NICHOLAS DEL ROSSO

I, **NICHOLAS DEL ROSSO**, of 1340 Environ Way, Chapel Hill, North Carolina, 27517 USA **WILL SAY** as follows:

1. I am the same Nicholas Del Rosso as provided a witness statement dated 21 June 2019 in support of the Claimant, Ras Al Khaimah Investment Authority ("**RAKIA**"), in the High Court proceedings to which this appeal relates and I gave evidence at the trial of these proceedings. I provide this witness statement to address certain matters arising out of the application made by the Defendant ("**Mr Azima**") on 12 February 2021 (the "**Application**").

2. I am the President and owner of Vital Management Services Inc. of the above address ("**VMS**"). VMS provides consulting services to law firms and businesses engaged in investigating or evaluating suspected fraud. Much of my work is undertaken in the context of litigation and nothing in this witness statement is intended to or should be taken as waiving any privilege in relation to the matters described.

3. Save insofar as is stated otherwise, the facts set out below are within my own knowledge or are derived from other sources or documents that I have seen and which in all cases I believe to be true. Where any facts are not within my knowledge, the source of those facts is stated.

4. There is shown to me and exhibited hereto a paginated bundle marked "NDR1". Unless otherwise stated, references to page numbers (shown in bold/square brackets) in this statement refer to the page numbers in NDR1.

5. As I made clear in the evidence I gave at the trial of these proceedings, I did not hack Mr Azima's computers, or arrange for anyone else to hack him. I do not know who hacked his computers. Similarly, I did not upload his data to the internet, cause his data to be uploaded or know who did upload his data.

6. It was not suggested at the trial that I had any role in hacking Mr Azima. However, on 13 October 2020 Mr Azima's US lawyer, Mr Kirby Behre, wrote to me alleging that I had been involved, demanding my cooperation and threatening me with litigation if I refused **[1 – 2]**. A draft complaint before the US Court was attached to Mr Behre's letter **[3 – 28]**. Mr Behre suggested that my cooperation with Mr Azima would "*not be valuable*" if I disclosed the draft complaint or the letter to anyone other than a lawyer. I did not respond to these demands and, on 15 October 2020, Mr Azima filed a complaint against me and VMS in the US District Court for the Middle District of North Carolina (the

"**Complaint**"). As has been stated in a declaration of my US counsel in the proceedings in North Carolina (to which a copy of Mr Behre's letter dated 13 October 2020 was exhibited), Mr Behre suggested in a call with my US counsel that the lawsuit against me could be resolved if I would cooperate with Mr Azima, stating that "*information was much more valuable than money*" **[29 – 33]**.

7. The Complaint alleges that I oversaw and directed the hacking of Mr Azima, having been engaged and paid to do so by Dechert LLP on behalf of RAKIA. It further alleges that I engaged the services of "*the Indian hacking firm"* CyberRoot Risk Advisory Private Limited ("**CyberRoot**") for this purpose. The Complaint alleges that VMS and I had paid CyberRoot more than $1 million for the hacking of Mr Azima and the dissemination of his stolen data. Six days after the Complaint was filed, Mr Azima sought the US District Court's permission to issue subpoenas against eight non-parties, including other witnesses in these proceedings, Dechert LLP, and Kotak Mahindra Bank. This request was denied by the US District Court on 14 December 2020. On 21 December 2020, VMS and I filed a motion to dismiss the Complaint. This has yet to be ruled on by the US District Court.

8. It is apparent from the Complaint and the application directed to Kotak Mahindra Bank that Mr Azima was aware in October 2020 that VMS had made payments, via that bank, to CyberRoot of more than $1 million. On 5 February 2021 an application was made by other litigants in the English courts to take discovery from me and VMS in aid of foreign proceedings under 28 USC §1782. In support of that application, these litigants relied on bank statements (which I refer to further at paragraph 13 below) which it seems were provided to them. That application has not yet been determined.

9. The statements made in the Complaint and in the material recently filed by Mr Azima in these proceedings to the effect that either I or VMS had any involvement in or knowledge of the hacking are categorically false. I have had no such involvement. Neither I nor VMS have ever commissioned, solicited or paid for any hacking of Mr Azima's computers. As explained below, all my dealings with CyberRoot were legitimate business transactions in the course of fraud investigations and related work being carried out for various clients. I am not aware of any evidence which suggests that CyberRoot carries out illegal hacking of any kind.

10. I have seen a copy of the witness statement of Jonas Rey dated 11 February 2021, which I am told by RAKIA's lawyers was filed with Mr Azima's Application. In that statement Mr Rey says he has been informed by a "Source" (that he does not name) that CyberRoot was responsible for the hacking of Mr Azima and the uploading of his data to the internet. He also says that he has been told by an individual named Vikash Pandey that CyberRoot was instructed to hack Mr Azima and Dr Massaad by me. Mr Rey says that he had been told by Mr Pandey that I requested CyberRoot to *"set up methods to monitor Mr Azima's ongoing emails"* and that VMS instructed CyberRoot to disseminate Mr Azima's hacked data online. This is completely untrue: neither I nor VMS did any of these things. I never engaged CyberRoot to carry out hacking or the dissemination of hacked data online. Furthermore, I have never dealt with or, prior to these allegations, heard of the individuals referred to in Mr Rey's witness statement as having allegedly been involved in the hacking of Mr Azima (that is, Messrs Vibhor Sharma, Rajat Shirish and Vikash Pandey).

11. As I made clear at the trial of these proceedings, the work that I did for Dechert LLP from early 2015 principally focused on the investigation in India of assets potentially stolen from RAKIA and/or the Government of

Ras Al Khaimah ("**RAK**"). I understand that Dechert was engaged to do this work by RAK Development LLC ("**RAK Development**"). India is a country that I know well and I had worked there prior to undertaking any work for Dechert or RAK. As I explain below, CyberRoot assisted me with some of this work. To be clear, however, the work I did in India did not relate to Mr Azima, and none of the work that CyberRoot has done for me related to Mr Azima.

12. I was first introduced to CyberRoot in 2014, when they assisted VMS with reputation management work for an unrelated client. I understood then and now that CyberRoot was a business providing information technology ("**IT**") and cyber security services, as well as online reputation management and digital forensics services, and that they were accredited to do work for the Indian government. It was never suggested to me that CyberRoot provided "hacking" facilities or was a "hack for hire" company, and I have never engaged them to "hack" or "phish" anything.

13. I am informed by RAKIA's lawyers that as part of his Application, Mr Azima seeks permission to rely on redacted documents that are said to be bank statements of CyberRoot from Kotak Mahindra Bank (exhibited to the Twelfth Witness Statement of Mr Holden ("**Holden 12**") as DPHR12 pages 557-566) ("**Exhibit G**"). These are not statements originating from any VMS account, and I have never seen these documents before, so I cannot attest to their authenticity. To the extent that Exhibit G contains confidential financial information, neither I nor VMS consented to its disclosure. I have been shown a table exhibited to Holden 12 which is said to list payments shown in Exhibit G as having been made by VMS to CyberRoot (DPHR12 pages 657-658) (the "**Table**").

14. For the avoidance of doubt, I confirm that none of the payments in the Table related to work that: (i) concerned Mr Azima; or (ii) involved any instructions to hack anyone or to disseminate material obtained through hacking. As I have already said, neither I nor VMS had any involvement in (or knowledge of) the hacking of Mr Azima. I would add that neither I nor VMS have ever instructed or had any dealings with any entity known as BellTrox (whether directly or indirectly) and as far as I am aware there is no affiliation between BellTroX and CyberRoot.

15. The payments listed in the Table related to the following:

    a. The first work I instructed CyberRoot to do was in 2015 and was to make sure that the computers and other electronic devices that were being used for the investigation work that VMS was undertaking for Dechert in India were secure from an IT perspective. CyberRoot provided assistance to the extent we encountered technical issues, including identifying potential malware on laptops. Payment 1 related to this work.

    b. I was happy with the work CyberRoot did as they were responsive and competent. As a result, following suspected data breaches of both data we had in India related to our investigations and data in RAK, in 2016 I instructed CyberRoot to undertake a data security audit and review exercise. This involved testing the security of systems and providing recommendations as to preventative measures that could be taken. During 2016 and early 2017, CyberRoot also assisted with investigatory work that was undertaken following further suspected data breaches. Payments 2, 3, 4, 8, 10, 13, 16, 17, 18, 19, 21, 29 and 30 were for this work. I believe that there is a typographical error in the Table insofar as it dates payment 3 as having been made on 15 March 2015, when it was in fact made on 15 March 2016 (which is consistent with Exhibit G).

c. During 2016 I also instructed CyberRoot in relation to ad hoc IT related issues that arose in the course of VMS and Dechert's investigation work for RAK Development, specifically forensic data recovery and analysing an IP address related to a suspected phishing attempt. Payments 9 and 15 related to such work.

d. In the latter part of 2016 and early 2017, CyberRoot performed some online reputation management work investigating sites containing material damaging to the reputation of individuals associated with RAK. Payments 20, 24, 25 and 26 were for this work.

e. The remaining 15 payments identified in the Table, payments 5, 6, 7, 11, 12, 14, 22, 23, 27, 28, 31, 32, 33, 34 and 35 were for work for clients other than RAK Development or RAKIA (and were, for the avoidance of doubt, unrelated to Mr Azima or Dr Massaad). This includes payments 11 and 12 which are specifically commented on in Holden 12. These payments were for an African client and concerned considerable online reputation management work for the client and that client's family, the details of which are confidential.

16. Since I received the Complaint, CyberRoot has provided to me a copy of a letter from Mr Azima's English solicitors Burlingtons dated 20 August 2020 addressed to Mr Pandey **[34 – 35]**. I understand from CyberRoot that they were provided the letter by Mr Pandey. It stated that Burlingtons was in possession of information which confirmed that Mr Pandey was involved in and was instrumental to hacking Mr Azima. The letter offered Mr Pandey a *"single opportunity to co-operate"* with Mr Azima by providing a witness statement.

17. I was also provided by CyberRoot with an email from Mr Holden to Mr Pandey (which again I understand CyberRoot was given by Mr Pandey) attaching a copy of a consultancy agreement dated 4 September 2020

signed by Mr Holden on behalf of Burlingtons (the "**Consultancy Agreement**") **[36 – 42]**. The Consultancy Agreement sought to engage Mr Pandey as a consultant to provide assistance to Burlingtons in relation to their investigation into the hacking of Mr Azima including by the giving of evidence. I note that the Consultancy Agreement provides for Mr Pandey to be paid $550 an hour and requires him to be available for meetings for up to 30 hours a month for 18 months.

STATEMENT OF TRUTH

I believe that the facts stated in this witness statement are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed.....

NICHOLAS DEL ROSSO

Date: 22 February 2021

Respondent/Claimant
N del Rosso
Second
NDR1
22 February 2021

IN THE COURT OF APPEAL **APPEAL REF: A3/2020/1271**

ON APPEAL FROM THE HIGH COURT OF JUSTICE HC-2016-002798

BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES

BUSINESS LIST (ChD)

BETWEEN:

RAS AL KHAIMAH INVESTMENT AUTHORITY

Respondent/Claimant

- and -

FARHAD AZIMA

Appellant/Defendant

EXHIBIT NDR1

This is the Exhibit marked "NDR1" referred to in the second witness statement of Nicholas del Rosso dated 22 February 2021.

Miller & Chevalier

Kirby Behre
Member
(202) 626-5960
kbehre@milchev.com

October 13, 2020

CONFIDENTIAL
OFFER OF SETTLEMENT UNDER FRE 408
WITHOUT PREJUDICE

Via E-mail

Nicholas Del Rosso
Vital Management Services Inc.
1340 Environ Way
Chapel Hill, North Carolina, 27517

Re: Your Involvement in the Hacking of Farhad Azima

Dear Mr. Del Rosso:

We represent Farhad Azima regarding the hacking he suffered. You testified at trial in the UK regarding the hacking of Mr. Azima and the distribution of his stolen data. Subsequently, we have learned that you were directly involved in the hacking, that you oversaw the work of CyberRoot Risk Advisory Private Limited to hack Mr. Azima on RAKIA's behalf, and that you testified falsely about these issues at the UK trial. You paid CyberRoot more than $1 million to steal Mr. Azima's data. Mr. Azima intends to file suit against you, and we write before doing so to offer you the opportunity to cooperate with us regarding this matter.

The attached draft complaint summarizes some, but not all, of the misconduct you and others were involved in relating to the hacking of Mr. Azima. Any complaint we file may include additional allegations, and similar lawsuits may be filed in other jurisdictions, including the UK. However, if you are willing to cooperate fully with us in recovering damages from those involved, we will consider releasing you from Mr. Azima's claims in all jurisdictions.

Your truthful cooperation will not be valuable to us if you disclose the attached draft complaint, this letter, or any information regarding our offer of settlement with anyone other than a lawyer if you choose to consult with one. If we reach an agreement regarding your cooperation,

we will ask that you confirm to us in writing that you (and any lawyer you retain, if you decide to retain one) have not shared this information with anyone.

If you are interested in discussing the possibility of cooperating with us, we must hear from you before 5 pm Eastern time on Thursday, October 15, 2020. Should you decide not to cooperate, our client will proceed to file suit without further notice.

Sincerely,

Kirby Behre

CC: Ian Herbert, Miller & Chevalier Chartered
Chris Jones, Womble Bond Dickinson
Ripley Rand, Womble Bond Dickinson

Enclosure

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

FARHAD AZIMA, 5921 Ward Parkway Kansas City, Missouri 64113, Plaintiff, v. NICHOLAS DEL ROSSO, VITAL MANAGEMENT SERVICES INC. , Defendants.	Civil Action No. XXXXXX

COMPLAINT

1. Plaintiff, Farhad Azima, by and through his undersigned counsel, files this Complaint against Nicholas Del Rosso ("Del Rosso") and Vital Management Services Inc. ("Vital"), and alleges as follows:

INTRODUCTION

2. Defendants Del Rosso and Vital oversaw and directed the hacking of Plaintiff Farhad Azima. Defendants stole Azima's computer data, including emails and trade secrets. The stolen data was then published online and used by Defendants and others, on behalf of the Ras Al Khaimah Investment Authority ("RAKIA"), in order to ruin Azima's reputation and damage him financially. Upon information and belief, Defendants were engaged and paid by Dechert LLP, which represented RAKIA in a dispute with Azima.

3. RAKIA, the state investment entity for the government of Ras Al Khaimah, hired individuals and companies, directly and through Dechert LLP, to investigate Azima, hack his

computers, steal his private data, and weaponize that data in an attempt to ruin Azima. Those individuals and companies included Stuart Page in the United Kingdom and the Defendants in the United States. Defendant Vital was hired by Dechert LLP through partner Neil Gerrard on behalf of RAKIA, and Defendants then hired CyberRoot Risk Advisory Private Limited ("CyberRoot") to provide the technical support necessary to hack Azima. CyberRoot is a company based out of Gurgaon, India that engages in illegal hacking. BellTroX Info Tech Services ("BellTroX") assisted CyberRoot in hacking Azima. BellTroX is a hacking company based in New Delhi, India. According to a June 9, 2020 press report by Thomson Reuters, BellTroX was involved in "one of the largest spy-for-hire operations ever exposed," helping clients spy on more than 10,000 email accounts over a period of seven years. On February 11, 2015, the founder and owner of BellTroX, Sumit Gupta, was indicted by the United States Department of Justice in the Northern District of California for hacking. Gupta remains at large.

4. In its investigation of 'hack-for-hire' organizations (including BellTroX), Thomson Reuters reviewed a cache of data revealing "tens of thousands of malicious messages designed to trick victims into giving up their passwords" – phishing and spear phishing emails – that BellTroX distributed between 2013 and 2020. Upon information and belief, the data cache revealed that email accounts belonging to Azima and his associates were among the accounts targeted by the BellTrox/CyberRoot phishing operation.

5. Defendants paid CyberRoot more than $1 million for the hacking of Azima and the dissemination of his stolen data. The work done by CyberRoot, assisted by Bell TroX, was done at the direction of the Defendants and others.

6. CyberRoot sent Azima phishing and spear-phishing emails, and successfully induced Azima to unwittingly provide them with passwords for his accounts. The successful hack gave

CyberRoot persistent access to Azima's computers and email accounts, and CyberRoot obtained real time access to Azima's emails. CyberRoot disclosed Azima's stolen data on internet blog sites they created. These blog sites contained links to BitTorrent sites and We Transfer sites, set up by CyberRoot, that contained at least some of the data Defendants and CyberRoot stole from Azima.

7. Defendants hacked Azima because they were hired to do so on behalf of RAKIA by Gerrard and Dechert LLP. Dechert LLP represented RAKIA in a dispute with Azima, and Gerrard wanted Azima's stolen data to use in a suit to be brought by RAKIA against Azima in England. Page, Del Rosso, Gerrard and RAKIA's manager James Buchanan created a false evidentiary trail to cover up their and RAKIA's responsibility for the hacking, and to suggest that Page had innocently found the hacked material on BitTorrents. RAKIA brought the lawsuit against Azima using the hacked material. The hacking was a defense raised by Azima, as well as forming the basis for a counterclaim by Azima.

8. The English court ruled that RAKIA, Page, and others had lied about how they obtained Azima's stolen data. Del Rosso gave a sworn witness statement in the U.K. suit, denying any knowledge of how the stolen emails were obtained. That witness statement was false. Del Rosso gave live, sworn testimony during the trial. That testimony was false as well. RAKIA's lawyers, including Dechert LLP, had also asserted (in formal correspondence, witness evidence and pleadings signed by those lawyers) that RAKIA had innocently discovered the materials on the internet. Those assertions were also false, given the Judge's ruling.

9. As a result of the conduct of Del Rosso, Vital, and their co-conspirators, Azima has suffered significant financial and reputational damage.

PARTIES

10. Plaintiff Farhad Azima is a U.S. citizen who resides and works in Kansas City, Missouri. He is a successful businessman who has owned and operated multiple aviation-related companies. Azima's businesses engage in interstate and foreign commerce. All of Azima's computers and servers were and are located in the United States.

11. Defendant Nicholas Del Rosso is the owner and sole employee of his company, Defendant Vital Management Services Inc. ("Vital"). Vital is a one-man private investigator company. Vital is located at 1340 Environ Way, Chapel Hill, North Carolina, 27517, and Del Rosso lives at 318 Lystra Preserve Drive, Chapel Hill, North Carolina 27517.

12. Defendant Del Rosso is the president and owner of Vital, and he is one of two shareholders of Vital, along with his wife.

FACTS

13. Dechert LLP and partner Neil Gerrard hired Del Rosso and Vital to "investigate assets potentially stolen from the Government of Ras Al Khaimah ("RAK")." Throughout the course of his work for Dechert LLP, which lasted from at least August 2014 until at least 2019, Del Rosso was instructed by Dechert LLP and Gerrard, as well as Dechert LLP partner David Hughes. Del Rosso communicated with lawyers from Dechert LLP on a "very regular basis." Del Rosso hired Chris Swecker, a North Carolina-based lawyer, to assist Defendants in their work for Gerrard and Dechert LLP.

Hacking of Azima at Del Rosso's Direction

14. Starting in early 2015, Gerrard, Page, Buchanan, and others agreed to attack Azima. The agreement is evidenced by a redacted internal "Project Update" report dated March 26, 2015, presented by Page to the Ruler of RAK and provided to Buchanan and others, as well as numerous emails between Gerrard, Buchanan, and their associates, some of which discussed the plan to

"target," "attack," and "go after" Azima using "another channel." Based on these emails, an English court concluded that the desire to attack Azima in the summer of 2015 "is clear." The Project Update report claimed Azima was part of a "US team" to publicize human rights abuses by RAK and Gerrard. The report stated that "[t]he campaign is not public yet, so we will be able to gather intelligence on their progress in order to monitor their activities and attempt to contain or ruin their plans." Gerrard admitted to reading this report.

15. Gerrard hired Del Rosso and Vital. Upon information and belief, Del Rosso was hired to target Azima and to obtain Azima's emails and confidential data, as well as for other purposes; and Page was retained to assist in the targeting of Azima, which upon information and belief included hacking Azima. Del Rosso hired the Indian hacking firm CyberRoot to provide the technical expertise to attempt to lure Azima into providing his login data, so that Defendants and their co-conspirators could have persistent access to Azima's accounts and computers. At least five employees of CyberRoot, including the CEO Vibhor Sharma, hacked Azima pursuant to Del Rosso's instructions. CyberRoot was assisted by BellTroX, which permitted CyberRoot to use BellTroX's infrastructure, including its server, to conduct the hacking. This work was done at the direction of the Defendants and others. CyberRoot and BellTroX share common employees. One such employee is Preeti Thapiyal, whose LinkedIn page lists his work as including the creation of "undetectable phishing Payloads."

16. CyberRoot, assisted by BellTroX, attempted to gain access to Azima's computers and accounts through phishing and spear-phishing emails. They sent Azima phishing emails to harvest his credentials and gain access to his email accounts and computers. Azima complied, and unwittingly enabled CyberRoot's hackers to gain access to Azima's email accounts and computers.

The breach of Azima's computer systems gave CyberRoot covert and persistent access to Azima's email accounts and computers.

17. CyberRoot, Del Rosso, Vital, and other co-conspirators, including Dechert LLP, Gerrard, and Page, obtained numerous confidential and protected trade secrets belonging to Azima and his companies, including but not limited to privileged and confidential legal communications and advice and confidential internal pricing lists relating to food transport for U.S. troops in Afghanistan.

Disclosure of Azima's Data at Del Rosso's Direction

18. Acting at Defendants' direction, CyberRoot created, uploaded, and transmitted multiple unauthorized copies of Azima's data. Upon information and belief, at least some of that data was provided to Del Rosso, who was located in the United States.

19. In late July 2016, Gerrard met with Azima and threatened him. Within days of Gerrard's meeting with Azima, CyberRoot, which was assisted by BellTroX, created blog sites on or about August 7, 2016, accusing Azima of fraud. During this same period, Del Rosso made significant payments to CyberRoot for their efforts.

20. The websites contained links to BitTorrent sites that Dechert LLP later admitted contained large quantities of Azima's stolen data. These BitTorrent links were posted by users named anjames and an_james, which are usernames associated with Sharma at CyberRoot. CyberRoot also used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data.

21. CyberRoot posted the data on the internet to create the misimpression that the data CyberRoot and Defendants stole from Azima were available to anyone who used the internet. CyberRoot created BitTorrent links that contained Azima's stolen data and those links were posted

on the blog sites alleging fraud by Azima. Page, Del Rosso, Gerrard, and an Israeli journalist, Majdi Halabi, created a false story and evidentiary trail to cover up their and RAKIA's responsibility for the hacking, and to suggest that Page had innocently found the hacked material on BitTorrents after being alerted to it by Halabi.

22. In fact, the data on the BitTorrent links were not accessible to the public because the "seeders"[1] necessary for the data to be downloaded were not available. Dechert LLP, and others acting at their direction, are the only persons or entities known to have obtained the data from the BitTorrent sites.

23. In May and June 2018, the blog sites were modified to include new links to WeTransfer sites that contained copies of Azima's stolen data.

24. CyberRoot regularly used WeTransfer links to transfer data to Vital. CyberRoot set up the WeTransfer account using the email account an_james@protonmail.ch.

25. In June 2019, the links on the blog sites were modified to include new WeTransfer links containing some of Azima's stolen data. These links, as with all the links to copies of Azima's stolen data, were not authorized by Azima.

26. Defendants paid CyberRoot more than $1 million for their hacking services and the distribution of Azima's stolen data. The payments were made by Del Rosso and Vital to CyberRoot's bank, Kotak Mahindra Bank. Substantial payments were made to CyberRoot around the time that Azima's stolen data was published online.

27. Upon information and belief, Defendants obtained the significant sums to pay CyberRoot from Dechert LLP, which had engaged the Defendants on behalf of RAKIA.

---

[1] A torrent seeder is a user who owns the file being made available online through the torrent system. Without a seeder, a file cannot be downloaded.

Lawsuit Against Azima and False Testimony About Discovery of Azima's Data

28. In September 2016, Dechert LLP's Hughes, on RAKIA's behalf, threatened to file a lawsuit in the U.K. against Azima and provided Azima's counsel with some of the emails that Defendants and CyberRoot stole from Azima. RAKIA, represented by Dechert LLP, sued Azima in England in September 2016 repeatedly relying on the data that Defendants stole from Azima.

29. During the January 22, 2020 trial in the U.K., Dechert LLP and RAKIA repeatedly changed their story about how Azima's stolen data was obtained. The English court ruled that the story put forward by RAKIA and others on their behalf about how they discovered the stolen data was false. Specifically, the court said that the story told by Page, Halabi, and others of innocent discovery of Azima's stolen data was "not true," involved "unexplained contradictions, inconsistencies, and implausible elements," and "was both internally inconsistent and inconsistent with the contemporaneous documents."[2] The English court said that "the true facts" about how Dechert LLP and others obtained Azima's stolen data still "have not been disclosed," despite them being required to do so. The untrue story of innocent discovery was advanced by RAKIA's agents. Former Dechert LLP partner Hughes signed a statement of truth for RAKIA advancing the story of innocent discovery. Others, including Gerrard, Buchanan, and Page, put forward witness statements and testimony that supported the story the court found to be untrue.

30. Del Rosso was an important part of RAKIA's false story of "innocent discovery" by Page of Azima's stolen data. For example, Gerrard and Del Rosso exchanged a series of emails on August 15 and 16, 2016, in which Gerrard purported to "break the news" of the discovery of the hacked material on websites. But other evidence showed that Del Rosso was aware of these

[2] *Ras Al Khaimah Investment Authority v. Farhad Azima*, [2020] EWHC 1327 (Ch).

websites at least a week earlier. The emails of August 15 and 16, 2016, between Gerrard and Del Rosso were clearly an attempt to lay a false "paper trail" of discovery.

31. In his witness statement, Del Rosso hid his engagement of CyberRoot and denied any involvement in the hacking. Because of Del Rosso's concealment of the true facts, of which he had knowledge, Azima did not learn of the role played by Del Rosso and Vital until recently.

JURISDICTION

32. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331. Some of Azima's claims arise under federal law, including the Wiretap Act (Counts 1 and 2) and misappropriation of trade secrets under the Defend Trade Secrets Act and the Economic Espionage Act (Count 3).

33. The Court has supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over Azima's other claims, since those other claims relate to the federal statutory claims in this action and form part of the same case or controversy under Article III of the United States Constitution.

34. Additionally, this Court has diversity subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because Azima and Defendants are from different states and the amount in controversy exceeds $75,000, exclusive of interest and costs.

35. The Court's jurisdiction over defendants comports with due process. The Court has personal jurisdiction over Defendants Del Rosso and Vital, who are domiciled or have their principle place of business in North Carolina. Del Rosso works at Vital in North Carolina and lives at 318 Lystra Preserve Drive, Chapel Hill, North Carolina 27517. Vital is based in North Carolina and is located at 1340 Environ Way, Chapel Hill, North Carolina, 27517.

VENUE

36. Venue is proper under 18 U.S.C. § 1965(a) because the Defendants transact their affairs in this Judicial District. Defendants Del Rosso and Vital both transact their affairs in Chapel Hill, North Carolina, with Azima's causes of action arising out of those North Carolina transactions.

37. Venue is also proper under 28 U.S.C. § 1391(b)(2) because this is a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred. Defendants conspired with others and coordinated their illegal campaign to hack Azima and publish his stolen data from their principle place of business in Chapel Hill, North Carolina.

38. Venue is also proper under 28 U.S.C. § 1391(b)(3) because this judicial district has personal jurisdiction over all defendants.

COUNT ONE (All Defendants)

I. Disclosure of Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(c) and 2520)

39. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

40. Under 18 U.S.C. § 2511(c), any person who "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication."

41. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

42. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce."

43. In violation of 18 U.S.C. § 2511(1)(c), Defendants Del Rosso and Vital intentionally disclosed wire and electronic communications of Azima knowing and/or having reason to know that the information was obtained through interception.

44. Defendants Del Rosso and Vital directed CyberRoot to intentionally disclose large quantities of Azima's intercepted data by instructing that the data be posted on BitTorrent and WeTransfer. Links to those BitTorrent and WeTransfer sites were added to the blog sites that CyberRoot created. CyberRoot worked with BellTroX and at the direction of the Defendants to conduct the hacking and post the intercepted data. The intercepted data included, among other things, business and personal electronic communications between Azima and others across the United States and around the world.

45. Defendants Del Rosso and Vital caused CyberRoot to hack Azima's computers and email accounts. The hack gave CyberRoot persistent access to Azima's computers and email accounts.

46. Defendants Del Rosso and Vital knew or had reason to know that the information published on the WeTransfer links was obtained through interception because Del Rosso, through Vital, gave the instructions to CyberRoot to intercept Azima's data and paid CyberRoot more than $1 million to conduct the hack and publish the stolen data. Defendants Del Rosso and Vital also knew or had reason to know that the information was obtained through interception because, among other reasons discussed above, it included large quantities of privileged, private, financially

sensitive and trade secrets data, including private email communications, banking documentation, and business plans, including confidential internal pricing lists relating to food transport for U.S. troops in Afghanistan.

47. As a result of the disclosure of Azima's intercepted data, Azima suffered damages. Since at least June 2018, the stolen data has continued to be publicly available on WeTransfer through links that were posted to the blog sites created by CyberRoot, resulting in more than $75,000 of statutory damages under 18 U.S.C. § 2520(c)(2)(B), and further monetary damages in an amount to be proven at trial. Upon information and belief, Defendants Del Rosso and Vital have made significant profits from the disclosure of Azima's data, having been paid large sums of money to disclose the stolen data to damage Azima. As a result of the continued disclosure of Azima's stolen data, Azima has suffered, and will continue to suffer, irreparable harm to his person, reputation, business, and community standing.

COUNT TWO (all Defendants)

II. Conspiracy to Disclose and Use Intercepted Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(d) and 2520, 18 U.S.C. § 371)

48. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

49. Defendants Del Rosso and Vital willfully, intentionally, and knowingly agreed and conspired with CyberRoot, Dechert LLP, Page, and others to disclose Azima's intercepted data in violation of 18 U.S.C. §§ 2511 and 2520. Among other things, Defendants Del Rosso and Vital agreed and conspired to intercept Azima's data through a phishing and spear-phishing campaign resulting in the hackers obtaining persistent access to Azima's computers and email accounts. Defendants Del Rosso and Vital paid more than $1 million for the interception of Azima's data.

Defendants Del Rosso and Vital also agreed and conspired to disclose the intercepted data by instructing CyberRoot to publish the data on blog sites that were created by CyberRoot. CyberRoot used BitTorrent and WeTransfer to send the stolen data to Defendants Del Rosso and Vital as well as other co-conspirators.

50. Defendants Del Rosso and Vital, with full knowledge that they were engaged in wrongful actions, took steps in furtherance of the conspiracy, including paying more than $1 million to the company that conducted the hacking, and later covering up the hacking through a story that the English court found to be false.

51. Azima has been injured and has suffered monetary damages as a result of Defendants' conspiratorial actions in an amount to be proven at trial. As a result of the Defendant's conspiracy to disclose and use Azima's intercepted data, Azima has suffered, and will continue to suffer, irreparable harm to his person, reputation, business, and community standing.

COUNT THREE (All Defendants)

III. Misappropriation of Trade Secrets, 18 U.S.C. §§ 1831, 1832, 1836

52. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

53. Federal law creates a cause of action against "[w]hoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains" trade secrets. 18 U.S.C. § 1832(a)(1).

54. Federal law imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). See § 1832(a)(5).

55. Federal law also creates a cause of action against "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret." 18 U.S.C. § 1831(a)(1).

56. Federal law imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" the offense listed in § 1831(a)(1). See § 1831(a)(5).

57. "An owner of a trade secret that is misappropriated may bring a civil action . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1).

58. Azima's email accounts stored trade secrets, including but not limited to highly confidential business plans and proposals, research supporting those plans and proposals (including costs and service projections), information concerning business strategies and opportunities, and contacts for important business relationships. These trade secrets are substantially valuable to Azima, in excess of $75,000, as will be proven at trial.

59. Azima stored trade secrets that were used in interstate and foreign commerce. Azima has taken and continues to take reasonable measures to keep this information secret. For example, Azima has always maintained his information on secured servers that are protected by passwords, firewalls, and antivirus software.

60. Azima's trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

61. Azima's trade secrets have significant value, resulting from substantial investment of time and resources.

62. Azima has made, and continues to make, efforts that are reasonable under the circumstances to maintain the secrecy of his trade secrets.

63. Defendants Del Rosso and Vital, along with CyberRoot, Dechert LLP, Page, and others, unlawfully conspired to take, appropriate, and obtain Azima's trade secrets without authorization, by means of a cyberattack against him. Defendants Del Rosso and Vital and their co-conspirators knew that Azima's email accounts contained trade secrets and intended to steal them in order to harm Azima.

64. Defendants Del Rosso and Vital improperly disclosed and misappropriated Azima's trade secrets without consent or authorization when they instructed CyberRoot to hack Azima, steal copies of his data, including trade secrets, and distribute the data through BitTorrent and WeTransfer links on blogs created by CyberRoot.

65. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Azima has suffered damages, which include, but are not limited to, loss of business goodwill, loss in the value of his trade secrets and confidential business information, and harm to Azima's business, in an amount to be proven at trial. *See* 18 U.S.C. § 1836(b)(3)(B)(i)(I). Defendants' acts of misappropriation have affected interstate commerce.

66. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Defendants Del Rosso and Vital have unjustly benefited from their possession of Azima's trade secrets. Upon information and belief, Defendants Del Rosso and Vital, who were engaged by Dechert LLP, were paid substantial sums of money by Dechert LLP to conspire to steal and misappropriate Azima's trade secrets.

67. Defendants' conduct was willful and malicious.

COUNT FOUR (All Defendants)

IV. Computer Trespass (N.C. Gen. Stat. § 14-458)

68. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

69. In violation of N.C. Gen. Stat § 14-458, Defendants Del Rosso and Vital directly and/or through their agents knowingly and without authorization or reasonable grounds used Azima's computer and computer network with the intent to make or cause to be made unauthorized copies of Plaintiff's computer data.

70. Defendants Del Rosso and Vital conspired with others to use Azima's computer and computer network without authorization to make copies of Plaintiff's trade secrets, confidential business information, and personal information and communications that would provide leverage over Plaintiff.

71. Defendants Del Rosso and Vital instructed CyberRoot to hack Azima's computer and computer network. At the direction of Defendants Del Rosso and Vital, CyberRoot, which worked with BellTroX, carried out the hack on Azima and gained access to Azima's computer and computer network. The breach of Azima's computer systems gave CyberRoot persistent access to Azima's email accounts and computers. Thus CyberRoot, acting at the direction of Defendants Del Rosso and Vital and others, regularly used Azima's computer and computer networks to make unauthorized copies of Azima's computer data, and Defendants Del Rosso and Vital caused these unauthorized copies to be made. Defendants Del Rosso and Vital paid CyberRoot more than $1 million for their hacking services.

COUNT FIVE (All Defendants)

V. Conversion (North Carolina Common Law)

72. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

73. Defendants directly and/or through their agents, knowingly and without authorization or reasonable grounds, wrongfully possessed and converted computer data, documents, spreadsheets, communications, and other files owned by the Plaintiff.

74. Under North Carolina law, conversion occurs when a defendant wrongfully possesses or converts property under the ownership of the Plaintiff.

75. Defendants conspired to wrongfully obtain possession of Plaintiff's computer data, documents, spreadsheets, communications, and other files owned by the Plaintiff.

76. As discussed in more detail above, Defendants Del Rosso and Vital instructed CyberRoot to hack Azima and make unauthorized copies of Azima's computer data. At the direction of Defendants Del Rosso and Vital, CyberRoot successfully hacked Azima and obtained persistent access to Azima's email accounts and computers. Thus CyberRoot, acting at the direction of Defendants Del Rosso and Vital and others, regularly used Azima's computer and computer networks to make unauthorized copies of Azima's computer data, and Defendants Del Rosso and Vital caused these unauthorized copies to be made. Defendants Del Rosso and Vital paid CyberRoot more than $1 million for their hacking services.

COUNT SIX (All Defendants)

VI. Identity Theft (N.C. Gen. Stat. § 14-113.20 and § 1-539.2(c))

77. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

78. Defendants directly and/or through their agents knowingly and without authorization or reasonable grounds, obtained, possessed, and used identifying information of Plaintiff with the intent to fraudulently represent that Defendants were the Plaintiff for the purposes of obtaining materials of value, benefit, and advantage.

79. Pursuant to N.C. Gen. Stat. § 14-113.20, "identifying information" is defined to include "passwords;" "electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names;" and "any other numbers or information that can be used to access a person's financial resources."

80. Defendants conspired with CyberRoot, Dechert LLP, Page, and others to obtain, possess, and use Plaintiff's identifying information – including electronic mail passwords – for the purposes of obtaining trade secrets, confidential business information, and personal information and communications that would provide leverage over Plaintiff.

81. At the direction of Del Rosso, Vital, and others, CyberRoot sent Azima phishing emails asking him to reset his password. Azima complied, and unwittingly permitted CyberRoot's hackers to gain access to Azima's email accounts and computers. The persistent access to Azima's email accounts and computers allowed CyberRoot, at the direction of Defendants Del Rosso and Vital, to use Azima's email addresses and passwords to obtain substantial quantities of Azima's private data, including trade secrets, confidential business information, and personal information and communications.

COUNT SEVEN (All Defendants)

VII. Publication of Personal Information (N.C. Gen. Stat. § 75-66)

82. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

83. Defendants knowingly broadcast or published personal information of Azima's over the internet with actual knowledge that Azima objected to any such disclosure and without Azima's consent or knowledge.

84. Defendants published Azima's private information on blog sites hosting WeTransfer links in May and June of 2018, and again in June of 2019.

85. This personal information included, among others, checking account numbers, passwords, and other numbers and information that can be used to access Azima's financial resources.

86. Among other documents, Defendants published financial transaction records, spreadsheets, business records, and banking information – all marked confidential.

87. Defendants' publication of Azima's personal information on the internet despite Azima's objection and without Azima's consent or knowledge directly and proximately caused actual injury to Plaintiff.

88. Azima is entitled to damages for each of Defendants' unlawful acts of publication of personal information in accordance with N.C. Gen. Stat. § 1-539.2(c).

COUNT EIGHT (All Defendants)

VIII. Violation of Trade Secrets Protection Act (N.C. Gen. Stat. § 66-153)

89. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

90. Azima's email accounts and computer systems contained business or technical information, formulas, patterns, programs, devices, compilations of information, methods, techniques, or processes. This information included highly confidential business plans and proposals, research supporting those plans and proposals (including costs and service projections),

information concerning business strategies and opportunities, and contacts for important business relationships. This information constituted trade secrets under Chapter 66 of the North Carolina General Statutes.

91. Azima derived independent actual or potential commercial value from these trade secrets not being generally known or readily ascertainable through independent development or reverse engineering by persons who can obtain economic value from their disclosure or use.

92. Azima has undertaken and continues to undertake reasonable efforts under the circumstances to maintain the secrecy of his trade secrets. For example, Plaintiff has always maintained his information on secured servers that are protected by passwords, firewalls, and antivirus software.

93. Azima's trade secrets are substantially valuable to Plaintiff, in excess of $75,000, as will be proven at trial.

94. Azima kept trade secrets that were used in interstate and foreign commerce.

95. Azima's trade secrets have significant value, resulting from substantial investment of time and resources. If known to Azima's competitors, Plaintiff's trade secrets would be of value to those competitors.

96. Azima's trade secrets included, among others, confidential internal price lists and confidential spreadsheets connected to contracts with the United States government to supply troops in Afghanistan.

97. Defendants Del Rosso and Vital, along with CyberRoot, Dechert LLP, Page, and others, unlawfully conspired to acquire, disclose, or use Azima's trade secrets without express or implied authority or consent by means of a cyberattack against Azima. Defendants Del Rosso and Vital and their co-conspirators knew that Azima's email accounts and computer systems contained

trade secrets and intended to steal them in order to harm Azima. Defendants did not arrive at Azima's trade secrets by means of independent development, reverse engineering, or by obtaining them from a person or entity with a right to disclose any of the trade secrets.

98. Defendants Del Rosso and Vital improperly acquired, disclosed, or used Azima's trade secrets without consent or authorization when they instructed CyberRoot to hack Azima, steal copies of his data, including trade secrets, and distribute the data through BitTorrent and WeTransfer links on blogs created by CyberRoot.

99. Defendants' conduct in acquiring, disclosing, or using Azima's trade secrets was willful and malicious and part of a deliberate, clandestine strategy to injure Azima.

100. Azima discovered that Defendants misappropriated his trade secrets on or about (date after an investigation that began after revelations at the UK trial, etc.).

101. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Azima has suffered damages, including but are not limited to loss of business goodwill, loss in the value of his trade secrets and confidential business information, and harm to Azima's business, in an amount to be proven at trial. Defendants' acts of misappropriation have affected interstate commerce.

102. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Defendants Del Rosso and Vital have unjustly benefited from their possession of Azima's trade secrets. Upon information and belief, Defendants Del Rosso and Vital, who were engaged by Dechert LLP, were paid substantial sums of money by Dechert LLP to conspire to misappropriate Azima's trade secrets.

103. Defendants' conduct in misappropriating Azima's trade secrets as described above directly and proximately caused actual injury to Azima.

104. Because Defendants' conduct was willful and malicious, Azima is entitled to punitive damages pursuant to N.C. Gen. Stat. § 66-154(c).

105. Because Defendants' conduct was willful and malicious, Azima is entitled to reasonable attorney's fees under N.C. Gen. Stat. § 66-154(d).

COUNT NINE (All Defendants)

IX. Unfair and Deceptive Trade Practices (N.C. Gen. Stat. § 75-1.1)

106. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

107. Defendants' conduct in sending Azima phishing and spear phishing emails in an effort to access his emails, computers, communications, confidential information, personal information, trade secrets, and other data constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

108. Defendants' conduct in accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other data without his consent or knowledge constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

109. Defendants' conduct in publishing or distributing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

110. Defendants committed conduct in or affecting commerce by (1) sending Azima phishing and spear phishing emails, (2) accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other data without his consent or

knowledge, and (3) publishing or distributing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet.

111. Defendants committed conduct that was unfair and deceptive by (1) sending Azima phishing and spear phishing emails, (2) accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other data, and (3) publishing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet.

112. Defendants' conduct in committing the unfair and deceptive acts or practices as described above was willful and malicious and part of a deliberate, clandestine strategy to injure Azima.

113. Defendants' conduct in committing the unfair and deceptive acts or practices as described above directly and proximately caused actual injury to Azima.

114. Plaintiff discovered that Defendants committed unfair and deceptive acts or practices that injured him on or about August 28, 2020 following an investigation.

115. Because Defendants' conduct constituted unfair and deceptive acts or practices under N.C. Gen. Stat. § 75-1.1, Plaintiff's damages should be trebled pursuant to N.C. Gen. Stat. § 75-16.

116. Because Defendants' conduct constituted unfair and deceptive acts or practices under N.C. Gen. Stat. § 75-1.1 and Defendants willfully and maliciously engaged in that conduct, Plaintiff is entitled to recover reasonable attorney's fees pursuant to N.C. Gen. Stat. § 75-16.1.

COUNT TEN (All Defendants)

X. Civil Conspiracy (North Carolina Common Law)

117. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

118. Defendants knowingly and without authorization or reasonable grounds, wrongfully entered an agreement to commit unlawful acts resulting in injury to Azima by conspirators pursuant to a common scheme of stealing Azima's confidential information to use against him.

119. Under North Carolina law, a civil conspiracy occurs when there is an agreement between two or more individuals to do an unlawful act or to do a lawful act in an unlawful way, resulting in injury to a plaintiff inflicted by one or more of the conspirators pursuant to a common scheme.

120. Defendants entered into an agreement with CyberRoot, Dechert LLP, and others.

121. Under this agreement, Defendants directed that CyberRoot send phishing emails to induce Azima to reveal his credentials. Defendants would then use Azima's credentials to gain access to Azima's confidential information and copy the information for widespread publication. Defendants paid CyberRoot more than $1 million for these actions. Upon information and belief, Defendants were contracted and paid by Dechert LLP, on behalf of RAKIA, to conduct the hacking.

122. Because of Defendants' successful and unlawful phishing campaign against Azima, Azima had confidential information publicly exposed, suffered harm to business relationships, and suffered misappropriation of numerous trade secrets.

123. Defendants, CyberRoot, Dechert LLP, and Page engaged in this conspiracy pursuant to a common scheme of damaging Azima and tarnishing his reputation.

PRAYER FOR RELIEF

On the basis of the foregoing, and such evidence as Plaintiff will present at trial, Plaintiff requests the entry of judgment in his favor and against Defendants on all counts of the Complaint and the award of the following relief:

1. Compensatory damages incurred by Plaintiffs as a result of the actions of Defendants, in an amount to be determined at trial.

2. Statutory damages, in an amount to be determined at trial, including treble damages and punitive damages.

3. A mandatory injunction requiring Defendants to remove and return of Plaintiff's data from any computers, servers, or websites.

4. A prohibitory injunction obligating Defendants to refrain in the future from committing tortious acts against Plaintiff.

5. Pre-judgment and post-judgment interest in the amounts and at the rates provided by law.

6. Costs and expenses, including reasonable attorney's fees, incurred by Plaintiff in this action and as a result of the actions of Defendants alleged herein.

7. Such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff Farhad Azima respectfully requests a trial by jury of all issues so triable.

Dated: October XX, 2020

Respectfully submitted,

/s/ Kirby D. Behre

Kirby D. Behre (*pro hac vice* pending)
Brian Hill (*pro hac vice* pending)
Tim O'Toole (*pro hac vice* pending)
Ian Herbert (*pro hac vice* pending)
Calvin Lee (*pro hac vice* pending)
Miller & Chevalier Chartered
900 16th Street, NW
Washington, D.C. 20006
Telephone: (202) 626-5800
Fax: (202) 626-5801
Email: kbehre@milchev.com

WOMBLE BOND DICKINSON (US) LLP

Christopher W. Jones
North Carolina Bar No. 27625

Ripley Rand
North Carolina Bar No. 22275
555 Fayetteville Street, Suite 1100
Raleigh, North Carolina 27601
Phone: 919-755-2100
Fax: 919-755-2150
Email: chris.jones@wbd-us.com
ripley.rand@wbd-us.com

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-CV-954-UA-JLW

FARHAD AZIMA,	)
Plaintiff,	)
v.	)
NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC.,	)
Defendants.	)

DECLARATION OF BRANDON S. NEUMAN
IN SUPPORT OF DEFENDANTS' RESPONSE IN OPPOSITION TO PLAINTIFF'S MOTION FOR LEAVE TO SERVE THIRD-PARTY SUBPOENAS BEFORE RULE 26(f) CONFERENCE

I, **Brandon S. Neuman**, pursuant to 28 U.S.C. § 1746, do hereby declare under penalty of perjury the following:

1. I am a partner of the law firm of Shanahan Law Group, PLLC, 128 East Hargett Street, Suite 300, Raleigh, North Carolina, 27601. I am a member in good standing of the Bars of the State of North Carolina, the State of California, and of this Court. Shanahan Law Group, PLLC is counsel to Defendants Nicholas Del Rosso and Vital Management Services, Inc., in this matter.

2. I attach hereto as **Exhibit 1** a true and correct copy of the Approved Judgment of the High Court of Justice Business and Property Courts of

England and Wales Business List (ChD) in Ras Al Khaimah Investment Authority v Farhad Azima, [2020] EWHC 1327 (Ch), dated May 22, 2020. The proceedings leading to this judgment (assigned claim number HC-2016-002798) are referred to herein as the "English Proceedings."

3. I attach hereto as **Exhibit 2** a true and correct copy of the Approved Addendum to Judgment of the High Court of Justice Business and Property Courts of England and Wales Business List (ChD) in the English Proceedings (Ras Al Khaimah Investment Authority v Farhad Azima, [2020] EWHC 1686 (Ch)), dated June 30, 2020.

4. I attach hereto as **Exhibit 3** a true and correct copy of the Order of the High Court of Justice Business and Property Courts of England and Wales Business List (ChD) in the English Proceedings, sealed on July 31, 2020.

5. I attach hereto as **Exhibit 4** a true and correct copy of the Order of the Court of Appeal, Civil Division in Ras Al Khaimah Investment Authority v Farhad Azima, dated September 9, 2020 (regarding Plaintiff Farhad Azima's ("Azima's") application for permission to appeal aspects of the English High Court's judgments dated May 22, and June 30, 2020).

6. I attach hereto as **Exhibit 5** a true and correct copy of Azima's Re-Re-Amended Defence and Counterclaim filed in the English Proceedings, dated August 16, 2019.

7. I attach hereto as **Exhibit 6** a true and correct copy of Azima's Defendant's Skeleton Argument for Trial filed in the English Proceedings, dated January 15, 2020.

8. I attach hereto as **Exhibit 7** a true and correct copy of Azima's Defendant's Closing Submissions filed in the English Proceedings, dated February 11, 2020.

9. I attach hereto as **Exhibit 8** a true and correct copy of the email, letter, and draft complaint sent by Azima's counsel who has "specially appeared" in this matter, Kirby D. Behre of Miller & Chevalier Chartered in Washington, D.C., to Mr. Del Rosso on October 13, 2020. [Dkt. No. 17.]

10. On October 26, 2020, I participated in a teleconference with Azima's counsel, Kirby D. Behre of Miller & Chevalier Chartered and Ripley Rand of Womble Bond Dickinson (US) LLP, and Shanahan Law Group lawyers Kieran Shanahan and Jeffrey Kelly, regarding the status of this matter. During this teleconference, counsel for Plaintiff agreed to an extension of Defendants' deadline to file their Motion to Dismiss but refused to consent to my request for a courtesy extension of time for Defendants to respond to Azima's Motion for Leave to Serve Third-Party Subpoenas Before Rule 26(f) Conference. Mr. Behre also declined to share any evidence supporting Azima's claims in this action. Mr. Behre suggested this action could be resolved if

Defendants would simply cooperate, stating that "information was much more valuable than money."

I declare under penalty of perjury that the foregoing is true and correct.

Executed on November 12, 2020 in Raleigh, North Carolina.

_____

Brandon S. Neuman

CERTIFICATE OF SERVICE

I hereby certify that on this 12th day of November, 2020, I electronically filed the foregoing **Declaration of Brandon S. Neuman in Support of Defendants' Opposition to Plaintiff's Motion for Leave to Serve Third-Party Subpoenas Before Rule 26(f) Conference** with the Clerk of the Court using the CM/ECF system, which will send electronic notification of filing to the following:

Jonathan D. Townsend
Christopher W. Jones
Ripley Rand
Womble Bond Dickinson (US) LLP
555 Fayetteville Street, Suite 1100
Raleigh, NC 27601
jonathan.townsend@wbd-us.com
ripley.rand@wbd-us.com
chris.jones@wbd-us.com

Calvin Lee
Ian Herbert
Brian Hill
Kirby D. Behre
Miller & Chevalier Chartered
900 16th Street, NW
Washington, D.C. 20006
clee@milchev.com
iherbert@milchev.com
bhill@milchev.com
kbehre@milchev.com

SHANAHAN LAW GROUP, PLLC

By: */s/ Brandon S. Neuman*
Kieran J. Shanahan, NCSB# 13329
Brandon S. Neuman, NCSB# 33590
Jeffrey M. Kelly, NCSB# 47269
Nathaniel J. Pencook, NCSB# 52339
128 E. Hargett Street, Suite 300
Raleigh, North Carolina 27601
Telephone: (919) 856-9494
Facsimile: (919) 856-9499
kieran@shanahanlawgroup.com
bneuman@shanahanlawgroup.com
jkelly@shanahanlawgroup.com
npencook@shanahanlawgroup.com
Counsel for Defendants

BURLINGTONS

MORE THAN LAW

Mr. Vikash Kumar Pandey
S/O Narmda Pasad Pandey, 272
N Pa Pasan, Pasan, Maharani
Laxmi Ward No 12, Kotma
Anuppur
Madhya Pradesh – 484336

Date: 20 August 2020
Our Ref: DH/AZI0003.2

Dear Sir,

RE: OUR CLIENT: MR. FARHAD AZIMA

We act for Mr. Farhad Azima.

Background

In August 2016, Mr. Azima's private and confidential data was published on the internet after it was illegally obtained by a cyber security hack (**"the Hack"**).

As a result of the dissemination of his data, he has suffered substantial damage to his reputation and earning potential. We estimate that his losses amount to in excess of $20,000,000.

Your role

We are in possession of information which confirms that you were involved and, indeed, were instrumental to the Hack. This is a very serious matter and you are liable to compensate Mr. Azima for the damage he has suffered as a result of the Hack.

We are however aware that you are not the sole player in the Hack and that you were performing your role on the instructions you had received from your client.

In the circumstances, we are offering you a single opportunity to co-operate with Mr. Azima's legal team to reveal the identity of the client who instructed you to hack Mr. Azima and to provide a Witness Statement sworn by a statement of truth explaining (1) your role in the Hack (2) the means by which the Hack occurred and (3) on whose instructions you were acting.

You have 3 days on receipt of this letter to respond to this request. If we have not received a satisfactory reply that you will co-operate willingly, our client will proceed with legal proceedings against you.

[redacted] 5 Stratford Place, London W1C 1AX

Representative offices:
Almaty, Geneva, Gibraltar, Malta, Moscow, St. Petersburg

Tel: +44 (0) 207 529 5420
Fax: +44 (0) 207 495 7450
DX: 82986 Mayfair
Web: www.burlingtons.legal

We urge you to take legal advice on the contents and effect of this letter.

All our client's rights and remedies are reserved.

Yours faithfully,

Dominic Holden

BURLINGTONS LEGAL LLP

Message

From: Dominic Holden [dominic.holden@burlingtons.legal]
Sent: 9/4/2020 1:35:34 PM
To: vikz.hax@gmail.com
Subject: Private, Confidential and Privileged - Subject to Contract
Attachments: 2020 09 04 Consultancy Agreement (signed by Burlingtons).pdf

Dear Vikash,

I attach our signed counterpart of the Consultancy Agreement.

Please could you sign and then return to me a copy of the complete signed version (scan and email is fine).

Please do not hesitate to telephone me to discuss – my contact details are below.

Kind regards,

Dominic Holden
Partner
Burlingtons

Tel: +44 (0) 207 529 5420
Mob: 07863174364
Email: dominic.holden@burlingtons.legal
Fax: +44 (0) 207 495 7450
DX: 82986 Mayfair

BURLINGTONS

5 Stratford Place, London, W1C 1AX

DATED 04 SEPTEMBER 2020

VIKASH KUMAR PANDEY

- and -

BURLINGTONS LEGAL LLP

CONSULTANCY AGREEMENT

AGREEMENT IS MADE ON 04 **..... SEPTEMBER 2020**

BETWEEN:

(1) **Vikash Kumar Pandey** of S/O Narmada Pasad Pandey, 272 N Pa Pasan, Pasan, Maharani Laxmi Ward No 12, Kotma Anuppur, Madhya Pradesh - 484336 (**"the Consultant"**); (**"the Consultant"**); and

(2) **Burlingtons Legal LLP** incorporated and registered in England & Wales with company number OC360876 whose registered office is at 5 Stratford Place, London W1C 1AX ("**Burlingtons**").

WHEREAS:

(A) The Consultant is an IT expert and ex-employee of Cyber Root Risk Advisory Private Limited (**"CR"**).

(B) Burlingtons are the English solicitors acting for Mr. Azima who is the Defendant, Counterclaimant and Proposed Appellant in proceedings commenced by Ras Al Khaimah Investment Authority ("**RAKIA**") in the High Court in London under Claim No. HC-2016-002798 (the "**RAKIA Proceedings**"). The RAKIA Proceedings concern, amongst other matters, the hacking of Mr. Azima's emails in around 2015 / 2016 (**"the Hack"**).

(C) The Consultant has agreed to provide assistance to Burlingtons in relation to their investigation into the Hack (**"the Hacking Investigation"**).

(D) It is understood that by assisting Burlingtons with the Hacking Investigation (**"the Purpose"**) the Consultant is risking his reputation within the IT industry and his personal security and that the Consultant may be required to incur substantial costs to ensure that his personal security is protected.

(E) The Consultant has dedicated time, and will need to dedicate further time, to providing information and assistance in connection with the Hacking Investigation. It is agreed that the Consultant will be engaged for the Purpose on the terms set out below.

IT IS AGREED:

1. **INTERPRETATION**

1.1 In this Agreement:

"**Commencement Date**" means 1 August 2020;

"**Confidential Information**" means confidential or secret information relating to Mr. Azima and / or the Hacking Investigation, including, without limitation, the existence and terms of this Agreement and any communications between Burlingtons (and / or its agents and / or advisers) and the Consultant;

"**Services**" means the services described in clause 3.

1.2 In this Agreement, any reference to a statutory provision is a reference to the provision from time to time renumbered, amended, re-enacted or consolidated.

1.3 In this Agreement, unless the context otherwise requires:

(a) references to clauses are to clauses of this Agreement; and

(b) the headings to the clauses are for convenience only and do not affect the Agreement's construction or interpretation.

2. **APPOINTMENT**

2.1 With effect from the Commencement Date, Burlingtons has engaged the Consultant to perform the Services.

3. **SERVICES**

3.1 During his engagement under this Agreement, the Consultant will give information and assistance to Burlingtons and / or its agents in connection with the Hacking Investigation.

3.2 The Consultant acknowledges that this could involve, but is not limited to, assisting in relation to any regulatory or legal process, preparing witness statements and giving evidence in person.

3.3 Without prejudice to the generality of clause 3.1, the Consultant shall make himself available for meetings for up to 30 hours per calendar month (via Zoom or other form of agreed upon video conferring platform), such meetings to take place at Burlington's request upon giving the Consultant at least 3 business days' notice; and

3.4 The Consultant represents, warrants and agrees that:

(a) any information or assistance provided to Burlingtons pursuant to this Agreement will be complete and accurate, and will be given truthfully to the best of the Consultant's knowledge and belief.

(b) he is a former employee of CR and has knowledge of the practices of the company.

(c) The execution, delivery and performance of this agreement will not conflict with:-

(i) Any law or regulation applicable to him; and / or

(ii) Any agreement or instrument binding upon him.

3.5 The Consultant shall indemnify Burlingtons against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred arising out of or in connection with:-

(a) Any breach of the warranties contained in clause 3.4.

(b) Any breach of this agreement.

(c) The enforcement of this agreement.

(d) Any claim made against Burlingtons by a third party arising out of or in connection with the provision of the Services.

3.6 It is agreed that no information or documentation (except as required by an order of a court of competent jurisdiction, or pursuant to any proper order or demand made by any competent authority or body where Burlingtons is under a legal or regulatory obligation to disclose the information and / or documentation) provided by the Consultant pursuant to this Agreement will be used by Burlingtons (on behalf of Mr. Azima) in support of any, action, claim, or prosecution against the Consultant in relation to his liability for the Hack.

4. **REMUNERATION**

4.1 Subject to the terms of this Agreement, Burlingtons shall pay the Consultant the sum of $550 per hour (exclusive of any applicable VAT) in consideration for the provision of the Services for a period of at least 18 months.

4.2 Subject to Burlingtons' prior written approval, Burlingtons shall reimburse all reasonable expenses properly and necessarily incurred by the Consultant in the course of this Agreement, subject to production of receipts or other appropriate evidence of payment.

4.3 The payment referred to at paragraph 4.1 shall include all work undertaken and assistance provided to Burlingtons by the Consultant to the date of this Agreement.

4.4 The period of service referred to at paragraph 4.1 may be extended by written agreement between the parties.

5. **CONFIDENTIAL INFORMATION**

5.1 The Consultant will not, except with the prior written consent of Burlingtons or pursuant to an order of a court of competent jurisdiction, or pursuant to any proper order or demand made by any competent authority or body where the Consultant is under a legal or regulatory obligation to make such disclosure, or to the Consultant's lawyers, auditors or insurers on terms which preserve confidentiality:

(a) disclose or communicate to any person, firm or company;

(b) cause unauthorised disclosure of; or

(c) otherwise make use of,

any Confidential Information that he has or may have acquired in the course of his engagement (whether before, on or after the date of this Agreement) and will use his best endeavours to prevent the unauthorised disclosure or publication of such information. This obligation survives the termination of this Agreement.

5.2 The obligations in clause 5.1 will cease if the relevant Confidential Information comes into the public domain other than through the Consultant's default or negligence.

6. **TERMINATION**

6.1 Upon the termination of this Agreement for whatever reason, the Consultant will deliver up all property and any documents or other information belonging to Burlingtons (and / or to Mr. Azima), including any Confidential Information, whether held electronically or in hard copy, which is in the Consultant's possession or under his control. The Consultant will not retain any copies of any such property, documents or information without written permission from Burlingtons.

6.2 The termination of this Agreement will not affect any of the provisions of this Agreement that are expressed to operate or have effect after its termination (including without limitation clause 5.1) and will not prejudice the exercise of any right or remedy of either party that has accrued prior to termination.

7. **STATUS**

7.1 The relationship of the Consultant to Burlingtons will be that of independent contractor and nothing in this Agreement shall render him an employee, worker, agent or partner of Burlingtons and the Consultant shall not hold himself out as such.

7.2 This Agreement constitutes a contract for the provision of services and not a contract of employment and accordingly the Consultant shall be fully responsible for and shall indemnify Burlingtons for and in respect of:

(a) any income tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the performance of the Services, where the recovery is not prohibited by law. The Consultant shall further indemnify Burlingtons against all reasonable costs, expenses and any penalty, fine or interest incurred or payable by Burlingtons in connection with or in consequence of any such liability, deduction, contribution, assessment or claim; and

(b) any liability arising from any employment-related claim or any claim based on worker status (including reasonable costs and expenses) brought by the Consultant against Burlingtons arising out of or in connection with the provision of the Services.

8. **MISCELLANEOUS**

8.1 This Agreement contains the entire agreement and understanding of the parties and supersedes all prior agreements, understandings or arrangements (both oral and written) relating to the subject matter of the same.

8.2 If a provision of this Agreement is found to be illegal, invalid or unenforceable, then to the extent it is illegal, invalid or unenforceable, that provision will be given no effect and will be treated as though it were not included in this Agreement, but the validity or enforceability of the remaining provisions of this Agreement will not be affected.

8.3 This Agreement may be entered into in any number of counterparts and any party may enter into this Agreement by executing any counterpart. A counterpart constitutes an original of this Agreement and all executed counterparts together have the same effect as if each party had executed the same document.

8.4 The parties do not intend by virtue of this Agreement to confer any rights on any third party pursuant to the provisions of the Contracts (Rights of Third Parties) Act 1999, except that any Group Company shall be entitled to enforce this Agreement.

9. **APPLICABLE LAW AND JURISDICTION**

9.1 Any dispute arising out of or in connection with this contract, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration under the LCIA Rules, which Rules are deemed to be incorporated by reference into this clause.

9.2 The number of arbitrators shall be one.

9.3 The seat, or legal place, of arbitration shall be London.

9.4 The language to be used in the arbitral proceedings shall be English.

9.5 The governing law of the contract shall be the substantive law of England & Wales.

Signed by **Burlingtons Legal LLP**)
)
)
)
)

Dominic Holden

Dominic Holden

Partner

04 September 2020

Signed by **Vikash Kumar Pandey**)
)
)
)
)